PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G07F 7/10

A1

(11) International Publication Number: WO 95/10823

(43) International Publication Date: 20 April 1995 (20.04.95)

(21) International Application Number: PCT/GB94/02250

(22) International Filing Date: 14 October 1994 (14.10.94)

(30) Priority Data:
9321357.7 15 October 1993 (15.10.93) GB

(71) Applicant: BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

(72) Inventors: BRADY, Patrick, Shaun; 3 Mostyn View, New Brighton, Minera, Wrexham, Clwyd (GB). KENNING, Michael, John; 9 Warrington Road, Ipswich, Suffolk IP1 3QU (GB). ROBERTS, David, Anthony; 7 Rowanhayes Close, Ipswich, Suffolk IP1 1UX (GB). SEMOS, Robert, Ernest, Vickers; 183 Longlands Road, Sidcup, Kent DA15 7LB (GB). STIRLAND, Mark, Jonathan; Albert Villa, Duckamere, Bramford, Ipswich IP8 4AH (GB). WARD, Richard, Beresford; Tangley Way, The Street, Witnesham, Ipswich, Suffolk IP6 9HG (GB).

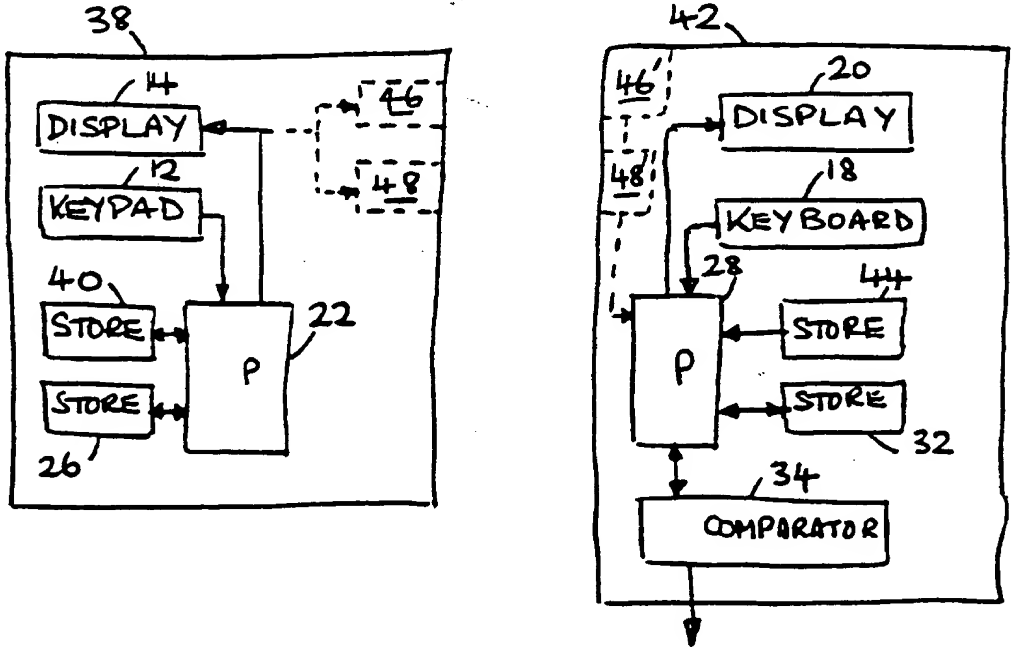
(74) Agent: SEMOS, Robert, Ernest, Vickers; BT Group Legal Services, Intellectual Property Dept., 13th floor, 151 Gower Street, London WC1E 6BA (GB).

(81) Designated States: CA, HU, JP, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

By Express Mail
No. EL470951471US

(54) Title: PERSONAL IDENTIFICATION SYSTEMS



(57) Abstract

In personal identification systems which compare passwords in a verification computer to identify a user, successive passwords are generated, or retrieved from a stored list in the verification computer in response to each entry of a public username into the verification computer. A user device carried by the user retrieves the next successive password from a stored list in response to a command from the user and displays the password. The user then reads this password and offers it to the verification computer via a keyboard entry to be compared with the password already generated or retrieved in response to the username (the expected password).

THIS PAGE BLANK (USPTO)

PERSONAL IDENTIFICATION SYSTEMS

The present invention relates to personal identification systems, and to user devices and verification computers for use therein.

A personal identification system is used to identify a person as having authority to access the entity or facility that is guarded by the system. Examples of such access include logging on to a computing system, control system or database, possibly via a telecommunications link, and entry to a room or building. Upon identifying a person, commonly called a user, the verification computer enables an access control means specific to the particular application.

It is known, for example from US patent No. 4,720,860, to generate passwords in accordance with a predetermined algorithm having a time dependent variable input provided by a digital clock which defines the variable as a function of the date and a predetermined interval of time. Thus the value of the variable input will change for each successive interval of time and in accordance with the actual value of time at, say, the start of each interval. Passwords are continually generated in a user device carried by an authorised user, the device having an internal clock which is initially synchronised with the internal clock of a verification computer. To gain a desired access via the verification computer, the user provides a public username to the verification computer followed by the password currently being generated by his user device. If this password matches a corresponding password generated by the verification computer in response to a recognised username and in accordance with its internal clock, the user is recognised or identified, and the access control means is enabled.

In accordance with a first aspect of the present invention, there is provided a method of identifying a user comprising the steps of communicating to a verification computer a public username and an offered password, the offered password being provided by a user device in the possession of the user and being or having been generated in accordance with a first predetermined algorithm having an input formed by a static variable, utilising in the verification computer the communicated username either to provide an expected password and to compare the communicated offered password with the expected password to identify the user upon the occurrence of a match, the expected password being or having been generated in accordance with the first predetermined algorithm with an expected value of the static variable, or to process the communicated offered password in accordance with the inverse of the first predetermined algorithm to obtain the value of the static variable corresponding to the communicated offered password and to compare the obtained value with the expected value of the static variable to identify the user upon the occurrence of a match, the expected value of the static variable of the utilising step being or having been generated directly or indirectly from the expected value corresponding to the last-occurring match (i.e. the most recent of any preceding matches) in accordance with a second predetermined algorithm.

Preferably, the second predetermined algorithm is or comprises a stepping function which steps the expected value corresponding to the last-occurring match to the next value in a predetermined sequence, herein referred to as sequence numbers.

More preferably, the offered password is either generated, or retrieved from a stored list of previously generated passwords, in response to receipt of a command signal by the user device and in accordance with the offered value of the static variable corresponding to the offered password being or having been generated directly or indirectly in accordance with the second predetermined algorithm from the value corresponding to the last-occurring offered password provided by the user device.

Preferably, when the verification computer comprises a stored list of expected passwords previously generated with the second predetermined algorithm providing sequence numbers as the static variable input to the first predetermined algorithm, there is included the step of providing the expected password comprising retrieving the password at the address constituted by the expected value of the static variable.

Preferably, when the user device comprises a stored list of offered passwords previously generated with the second predetermined algorithm providing sequence numbers as the static variable input to the first predetermined algorithm, there is included the step of providing an offered password comprising retrieving the password at the address constituted by a sequence number generated by the second predetermined algorithm in response to a received command signal or by the number communicated from the verification computer.

More preferably, there are included the prior steps, upon authorisation of a new user, of generating a respective random number, and generating the respective list of passwords to be stored in a user device to be issued to the newly authorised user starting with the random number as the first of the sequence numbers, entering the generated list of passwords into a store in the user device with the first password so generated being stored in the first location of the store, and issuing the user device to the newly authorised user; the generation of the expected static variable by the verification computer is constituted by entering the respective random number as the first of the sequence numbers in a respective store and replacing the current contents of the respective store with the next sequence number on each match of passwords for the respective user; and an offered password is retrieved from the location in the stored list of passwords in the user device corresponding to a running total of received command signals.

Preferably, the command signal is constituted by a predetermined input to the user device.

More preferably, the predetermined input is actuation of one or more specific keys of the user device.

Alternatively, the predetermined input comprises the entering of a first personal identification number (PIN) into the user device which matches a stored PIN therein.

In another alternative, the predetermined input comprises the entering of a username which matches a stored username therein.

Preferably, the user device provides the offered password via a display, and including entering a second personal identification number (PIN) into the user device and enabling the display upon matching the entered second PIN with a PIN stored in the user device.

As appropriate, preferably, the first PIN constitutes the second PIN .

Preferably, the first predetermined algorithm has a further input formed by a user-specific code.

More preferably there are included steps of storing the user-specific code in the verification computer, and retrieving the user-specific code for generating an expected password upon communication to the verification computer of a third personal identification number (PIN) which matches a stored PIN therein.

More preferably there are included steps of storing in the user device a predetermined code for use as the further input, and storing the predetermined code in the verification computer, said predetermined input comprising the entering of a further PIN into the user device which matches a corresponding PIN stored in the user device, and directly or indirectly comparing the communicated password in the verification computer with an expected password generated with the predetermined code as the further input, and actuating an alarm upon the occurrence of a match.

In appropriate embodiments, preferably the entering of any PIN other than said first PIN and, as the case may be, said further PIN, causes the user device to provide a password from a predetermined set of passwords not generated in accordance with the first predetermined algorithm and which the verification computer will recognise as resulting from unauthorised use of the user device and take no action.

More preferably, the user device delays the provision of the password from said predetermined set with progressively increasing delay for each such unauthorised use of the user device.

In embodiments having a user-specific code input, preferably there are included the steps of previously modifying the user-specific code in accordance with a fourth personal identification number (PIN) and a third predetermined algorithm, storing the PIN-modified user-specific code in the verification computer, communicating a fifth PIN to the verification computer, and utilising the inverse of the third predetermined algorithm and the fifth PIN to produce a code for use as said further input to the first predetermined algorithm, the correct user-specific code being produced only when the fifth PIN is the same as the fourth PIN.

Preferably, the user communicates the third PIN or the fifth PIN, as the case may be, directly to the verification computer.

Alternatively, the third PIN or the fifth PIN may be communicated to the verification computer from the user device.

Preferably, when the user device modifies the password to be offered in accordance with the third PIN or the fifth PIN and a fourth predetermined algorithm, the step of communicating the PIN to the verification computer is constituted by communicating the PIN-modified password to the verification computer and utilising therein the inverse of the fourth predetermined algorithm to obtain the communicated PIN.

Preferably, when the expected and offered passwords are generated as modified passwords in accordance with a fifth predetermined algorithm and a respective sixth and seventh personal identification numbers (PIN), the verification computer identifies the user on the basis of the comparison of the PIN-modified expected password with the communicated PIN-modified offered password.

The third, fifth or seventh PIN, as the case may be, may be stored in the user device. Alternatively, the user may enter the third, fifth or seventh PIN, as the case may be, into the user device.

As appropriate, the third, fifth or seventh PIN may be constituted by the first or second PIN, as the case may be.

Preferably, there are included the further steps, for identifying the verification computer to the user, of providing the next following expected password upon the occurrence of matching passwords, and comparing the next following expected password with the next following offered password provided by the user device.

Preferably, there are included the further steps of communicating the next following password directly to the user device, comparing it with the next following offered password in the user device and providing an indication of a match to the user.

Preferably, if the result of direct or indirect comparison of passwords is not a match, the verification computer deems the offered and expected static variables to be out of synchronism and makes up to a predetermined number of further comparisons with successive following expected static variables to attempt to resynchronise the expected static variable with the offered static variable.

According to a second aspect of the present invention there is provided a method of verifying a user comprising the steps of communicating to a verification computer a public username and offered verification information, herein referred to as OVI, utilising in the verification computer the communicated username to provide expected verification information, herein referred to as EVI, and comparing the communicated OVI directly or indirectly with the EVI, the verification computer accepting the user as identified if the comparison result is a match, the OVI being provided by a user device in the possession of the user and being obtained in accordance with a first predetermined process, and the EVI being obtained in accordance with a second predetermined process, the method being characterised by either the OVI being or having been generated from static information associated with verification information last provided by the user device, and the EVI being or having been generated from static information associated with verification information last used by the verification computer successfully to identify the user.

According to a third aspect of the present invention there is provided a user device for use in a personal identification system, the device comprising means for storing a list of passwords, means responsive to receipt of a command signal for retrieving, in use, a password from the storing means, and means for providing the retrieved password, in use, to a verification computer of the system.

Preferably, the retrieving means comprises means for counting the received command signals and means responsive to the counting means for addressing the storing means.

More preferably, the addressing means provides an address pointer which is equal to the current count of the counting means.

According to a fourth aspect of the present invention there is provided a user device for use in a personal identification system, the device comprising means for generating in response to receipt of a command signal a password to be offered, in use, to a verification computer of the system, and means for providing the generated password, in use, to the verification computer, the generating means being arranged to generate the password in accordance with a first predetermined algorithm having an input formed by a variable.

Preferably, the generating means is arranged to generate the password in accordance with a user-specific code forming a further input to the first predetermined algorithm.

More preferably, the generating means comprises means for counting received command signals and for supplying the current count as the variable input for the first predetermined algorithm.

Alternatively, the generating means comprises means for counting received command signals and is arranged to generate the variable input in accordance with a second predetermined algorithm having an input formed by the current count of the counting means.

Preferably, a user device comprises key means operable by a user to provide a signal constituting said command signal.

As appropriate, a user device may comprise first input means for plural character input, first means for storing a character stream, and first means responsive in use to the input of a character stream matching a first predetermined character stream stored in the first storing means for providing a signal which signal constitutes the command signal.

Appropriate user devices may comprise input means operable by a user for inputting a command signal comprising a number, and the retrieving means or the generating means, as the case may be, may be responsive to the command signal which it utilises as an address pointer or as the variable input.

Preferably, the providing means comprises means for displaying the retrieved or generated password.

In user devices having an abovementioned key means, preferably the displaying means is responsive to an enabling signal and comprises second input means for plural character input, second means for storing a character stream, and second means responsible in use to the input of a character stream matching a second predetermined character stream stored in the second storing means for providing a signal, which signal constitutes the enabling signal.

The abovementioned second input means, the second means for storing, and the second means for providing a signal, may be respectively constituted by the first input means, the first means for storing, and the first means for providing a signal.

Preferably, the providing means comprises means for communicating, in use, directly with the verification computer.

More preferably, a user device may comprise means for modifying a password to be provided in accordance with a predetermined algorithm having as inputs the password and a third predetermined character stream.

A user device may further comprise a third storing means for storing in use the third predetermined character stream, and wherein the modifying means is arranged to retrieve the third predetermined character stream from the third storing means.

The abovementioned third storing means may be constituted by the first storing means or the second storing means, as the case may be.

According to a fifth aspect of the present invention there is provided a verification computer for use in a personal identification system, comprising input means for receiving plural characters, means responsive to the receipt via the input means of a first predetermined character string, constituting a predetermined user name, for providing an expected password, means responsive to the receipt via the input means of a second predetermined character string, at least a part of which constitutes an offered password, for comparing the offered and expected passwords and for providing an indication in the event of a match, and means for counting said indications, and wherein the providing means comprises means for storing a list of passwords and means responsive directly or indirectly to the current count of the counting means for retrieving, in use, a password from the storing means.

Preferably the retrieving means provides an address pointer in accordance with a predetermined algorithm having an input formed by the current count of the counting means.

More preferably, the retrieving means comprises a look-up table generated in accordance with the predetermined algorithm and is arranged to address the table with the current count to retrieve the corresponding address pointer.

According to a sixth aspect of the present invention there is provided a verification computer for use in a personal identification system, comprising input means for receiving plural characters, means responsive to the receipt via the input means of a first predetermined character string, constituting a predetermined user name, for providing an expected password, means responsive to the receipt via the input means of a second predetermined character string, at least a part of which constitutes an offered password, for comparing the offered and expected passwords and for providing an indication in the event of a match, and means for counting the indications, and wherein the providing means comprises means for generating the expected password in accordance with a predetermined algorithm having a variable input formed directly or indirectly by the current count of the counting means.

Preferably, the generating means is arranged to generate the password in accordance with a user-specific code forming a further input to the predetermined algorithm.

More preferably, the providing means comprises means for storing the user-specific code and a corresponding predetermined character stream, and is arranged to retrieve and supply the user-specific code to the generating means upon an offered character string matching the corresponding predetermined character string.

More preferably, the offered character string is received via the input means. Alternatively, the providing means includes means for processing the second predetermined string in accordance with a further predetermined algorithm to produce the offered password and the offered character string.

Preferably, the providing means is arranged to provide the variable input indirectly in accordance with a predetermined algorithm having an input formed by the current count of the counting means.

More preferably, the providing means comprises a look-up table generated in accordance with the predetermined algorithm and is arranged to address the table with the current count to retrieve the corresponding variable value.

The input means may be arranged for direct communication from a user device forming part of the system.

The providing means may comprise output means for outputting character strings.

Preferably, the output means comprises a visual display.

The output means may be arranged for direct communication with a user device forming part of the system.

Preferably, the providing means is arranged to respond to said indication to provide the next following expected password corresponding to the next successive count value and to supply said next following expected password to the output means.

Embodiments of personal identification systems in accordance with the present invention will now be described by way of example with reference to the drawings, in which:

Figure 1 is a schematic diagram of a first embodiment of a personal identification system of the present invention;

Figure 2 is a schematic diagram of a second embodiment of a personal identification system of the present invention; and

Figure 3 is a schematic diagram of a modified form of the user device of the personal identification system of Figure 1.

In Figure 1 a personal identification system comprises a user device 10 having a pressure sensitive keypad 12 for numeric input and an LCD display 14, and a verification computer 16 having a keyboard 18 for alphanumeric input and an LCD display 20. User device 10 has substantially the same dimensions as those of a present-day credit card-sized calculator and further comprises a processor 22 with associated stores 24 and 26 containing a secret user-specific code (USC) and a sequence number, respectively.

The verification computer 16 comprises a corresponding processor 28 with corresponding associated stores 30 and 32 containing respective USCs and sequence numbers for the users to be identified by the system.

Upon communication of a user's username (UN) to the verification computer 16, in this embodiment by the user keying in his UN on the keyboard 18, the processor 28 checks the UN against a store of authorised UNs, and if the UN is recognised, reads from stores 30 and 32 the respective USC and sequence number corresponding to the input UN, and processes them as static variable inputs in accordance with a predetermined algorithm (also referred to as a process) to produce an expected password. As used herein the term "password" does not imply that a password has to be kept secret, since each is used once only and the next following password cannot be generated from a current password unless the impersonator knows at least the algorithm, the user-specific code and the current value of the static variable. Furthermore, the term "username" means any combination of alphanumeric characters, i.e. letters and/or numbers, which the verification computer will recognise as being associated with a purported known user. Where the user device is to be used in conjunction with, for example, a credit card, the username can be the user's account number.

Upon actuation of a predetermined one of the keys (a NEXT key) of keypad 12 by the user (i.e. providing a command signal), the processor 22 reads the contents of stores 24 and 26, processes them in accordance with the same predetermined stored algorithm to produce a password, and displays the password on the LCD display 14. This password will be referred to as an offered password.

The user reads the offered password displayed on his user device and keys this into the verification computer 16 via the keyboard 18 following the input of his UN. The verification computer 16 now makes a comparison of the expected and offered passwords using comparator 34 which provides an enabling signal on its output if the two passwords are identical, thus signifying that the user has been identified as having authority for the access that the personal identification system is guarding, and the enabling signal will be coupled to an appropriate access control means 36.

The predetermined algorithm is arranged such that after the sequence number has been read from store 26 (and 32), the number is incremented and written back into the store 26 (and 32) to replace the stored sequence number.

It will be understood that one of the necessary conditions for identical expected and offered passwords is that the respective sequence numbers must be identical. If a user actuates his user device 10 and does not make a corresponding entry for his UN into the verification computer 16, say through accidental actuation of the user device 10, the sequence number in store 26 will be greater than that in store 32. To allow for this possibility, if the comparator 34 does not provide the enabling signal upon comparison of the expected and offered passwords, the processor 28 proceeds to increment the sequence number in store 32 and perform another comparison with the offered password. If there has been no successful comparison (match) for five successive increments of the sequence number processor 28 will decrement the sequence number five times to restore the sequence number in store 32 to its original value. On the other hand, if there is a match then processor 28 simply increments the current sequence number to re-synchronise the user device 10 and verification computer 16.

Instead of incrementing and decrementing the sequence number in store 32 in the event of no match, the sequence number can be written into a further store for the purpose of incrementing and trying a new comparison. If there is a match then the value in the further store is written into store 32 and then incremented. If there is no match then the processor leaves the stores as they are because at the next "no match" the value in store 32 will overwrite the value in the further store.

In Figure 2, which shows an alternative embodiment of a personal identification system of the present invention, a user device 38 comprises the same elements as user device 10 except that: store 24 is replaced by a large capacity store 40 containing a list of passwords previously generated in accordance with the predetermined algorithm, the USC, and a series of consecutive sequence numbers; store 26 contains a pointer to the next password location to be read; and processor 22, upon actuation of the user device 10, reads the pointer value from store 26, reads the password from the corresponding location in store 40, displays this on the LCD display 14 as the offered password, increments the value of the pointer and writes this into store 26. In this embodiment processor 22 does not process any inputs in accordance with a stored algorithm but merely reads a stored password and displays it.

The number of passwords stored in store 40 will depend on the expected lifetime of the user device, including unintentional actuations, and can be several thousands.

Also shown in Figure 2, is a verification computer 42 which similarly comprises the same elements as verification computer 16 with the exception that store 30 is replaced by a large capacity store 44 containing for each user to be identified a respective list of passwords previously generated in accordance with the predetermined algorithm, the respective USC, and a series of consecutive sequence numbers, that store 32 contains respective current pointers for the users, and that processor 28, upon communication of a recognised UN, reads the respective pointer value from store 32, reads the corresponding password from the corresponding location in store 44 (the expected password), and passes it to the comparator 34, and increments the value of the pointer and writes this into store 32. Processor 28 similarly does not have a stored algorithm for processing a USC and sequence number.

When a person first becomes an authorised user, the verification computer generates a random number which it enters as the newly authorised user's respective pointer in store 32. This random number is also entered into store 26 of a user device before it is issued to the newly authorised user whereby the user device and the verification computer start in synchronism, because they both have the same initial value of pointer.

The list stored in store 40 need not have been generated starting with the lowest (first) value of the sequence numbers. Instead, and preferably, the list can be generated taking into account the random number (offset) assigned to the new user such that the first of the previously generated passwords, i.e. that corresponding to use of the offset as the static variable, will be stored in location number 1 of store 24. The previously generated list of passwords can be downloaded into store 40 in any suitable manner as is known in the art.

By starting this previous generation using the offset, srore 26 does not have the offset stored in it, but starts with the number 1. Thus upon first actuation, processor 22 retrieves this from store 26 and uses it as an address pointer to retrieve the password from the first location in store 40. The number in store 26 is then incremented to point to the second location, ready for the next actuation. Alternatively, the processor 22 can be arranged to increment the store 26 upon actuation rather than after retrieval of a password from store 40. In this case the store 26 can start empty. Whichever method is used in the user device, if a system has (as mentioned below) a verification computer 16, this will start with the offset in the respective location in store 32 and increment the offset after it has been used to generate the first password, and similarly increment it after each such generation.

It will be appreciated that user device 10 can be used in conjunction with verification computer 42, and that user device 38 can be used in conjunction with verification computer 16.

Instead of the communication of the offered password from user device 10, 38 being indirect via the user and keyboard 18, it may be direct by means of contacts 46 or a transmitter 48 (rf, acoustic, using DTMF tones, or ultrasonic), shown in dashed lines in Figure 2. Verification computer 42 will have corresponding contacts 46′ or receiver 48′ instead of or in addition to the keyboard 18.

In the modified user device 10′ in Figure 3, there is a further store 52 and a comparator 54. When the user first receives the user device 10′ he has to input via the keypad 12 a personal identification number (PIN) which is stored in store 52. The output of comparator 54 is used to inhibit the response of the processor 22 to the signal from the NEXT key until the correct PIN is input. In alternative arrangements, the output of comparator 54 is used to inhibit the LCD display 14, or the sending of the offered password to the display 14, and/or it is used to provide the offered password whereby the entering of the correct PIN constitutes a command signal for the user device.

The further store 52 and comparator 54 could be included in the user device 38, if desired.

In a modification of the above systems, the verification computer 16, 42 requires the receipt of a PIN which it checks against a respective stored value of PIN for the input UN, and actuation of the access control means 36 requires the correct PIN and the correct offered password. The user can enter this PIN at the keyboard 18. In a variant this PIN is held in storage in the user device 10, 10′, 38 and communicated directly or indirectly from it to the verification computer 16, 42. In a further modification processor 22 combines a stored PIN with the generated or retrieved password in accordance with a combining algorithm to produce a PIN-modified offered password. In the verification computer 16, 42 processor 28 combines the value of the stored PIN with the expected password in accordance with the same combining algorithm to produce a PIN-modified expected password and the two passwords are compared by comparator 34. In a variant of the verification computer 16, 42 the processor 28 processes the received PIN-modified offered password to produce the offered PIN and the offered password which are then respectively compared with the stored PIN and the expected password. The stored PIN can be the same as or different from the PIN used to enable the user device 10'.

In a modification of the user device 10', store 52 is arranged to store a first PIN for normal use, and a second PIN for abnormal use (e.g. use under duress), and the processor 22 is arranged to combine the matched first or second PIN with the generated password. The verification computer will detect whether the first (normal) PIN is used, or whether the user has input the second (duress) PIN to alert the verification computer to the situation and actuate an alarm. The processor is also arranged to respond to any PIN other than the first and second PINs by providing the next password in sequence from a predetermined set of passwords (e.g. twenty special passwords) which the verification computer will recognise as unauthorised use of the user device. The processor takes a progressively longer time to provide the password as more unauthorised attempts are made, e.g. several minutes, so as to inconvenience the unauthorised user. When the verification computer recognises any of the special passwords it takes no action.

The above described identification method can be extended such that after the verification computer 16, 42 has identified (authenticated) the user, it then generates or retrieves the next password and communicates it to the user via the LCD display 20 for mutual authentication. The user actuates his user device 10, 10', 38 to obtain the next offered password (or reads the next password from user device 56) and mentally checks that they are the same.

Where a user device can communicate an offered password directly to the verification computer, say by contacts, the mutual authentication process can be automatic if the processor 22 is arranged to receive the next password from the verification computer via the contacts to perform a comparison and to display a predetermined group of characters on the LCD display 14 to indicate the result of the mutual verification process. Depending on the programming of processor 22 the characters can be alphanumeric or numeric. Alternatively, or additionally, authentication of the verification computer can be indicated to the user by an acoustic signal.

The above described personal identification systems can be used to guard access to computer terminals in a wide variety of circumstances where secure access is required. The access can be remote via a telecommunications link, via modems if required. The systems can be used to guard access to buildings, rooms and the like, in this case the access control means 36 is arranged to unlock a door or the like to give the user access to the guarded property.

In alternative embodiments of systems in accordance with the present invention the processor 28 in verification computer 42 is arranged to respond to the input of a UN to convert, in accordance with a further algorithm (preferably a pseudo random number generator), the value of the running total of successful UN inputs (i.e. those which result in a match of offered and expected passwords) into a substitute value to be used as the pointer and write it into store 32. The verification computer obtains the expected stored password from the store location corresponding to the pointer stored in store 32.

Instead of generating the substitute value for the pointer in response to the input of the UN, the processor 28 can generate and store the substitute value at the conclusion of a password match, and merely respond to the UN input by reading store 32.

It will be understood that in such embodiments the substitute value for the pointer in the verification computer can be previously generated and held in store or can be generated in real time, independently of whether the expected passwords are previously generated and held in store or are generated in real time. Similarly, in user devices which utilise a running total of received command signals a corresponding substituted pointer value can be previously generated by the further algorithm and held in store or can be generated in real time by the further algorithm, independently of whether the offered passwords are previously generated and held in store or are generated in real time.

It will be appreciated that a username can be any combination of alphanumeric characters, as is known in the art, and that if desired actuation of the user device can be by entering a username, keypad 12 being arranged for alpha characters as well as or instead of numeric characters, as the case may be, and that if a lower level of security is acceptable, then the USC input to the predetermined algorithm can be omitted.

Instead of generating, or retrieving, a password in response to a UN input or a command signal, the processor in the user device and/or the verification computer can generate or retrieve the next expected/offered password and put it into a store in readiness for the next access attempt.

It will be appreciated that the abovedescribed methods are not limited to identifying the user at an initial point of entry to a system etc., but can also be used to identify the user to a remote destination, for example the password can be appended to the end of an electronic message to verify to the recipient the alleged sender of the message, the verification being performed by the destination terminal.

It is expected that the user will usually be human, but it is envisaged that non-human forms, for example robotic forms and intelligent terminals, can use such a method to identify themselves.

In the abovedescribed embodiments the verification computer compares two independently obtained passwords each of which is or has been generated by use of the same predetermined algorithm. The present invention also embraces methods and systems in which the verification computer processes the received offered password in accordance with the inverse of the algorithm with which it was generated and thus obtains the value(s) of the input(s) used in the generation of the offered password and makes a comparison with an expected value(s) for such input(s).

As described above, the verification computer generates a static variable input for the predetermined algorithm as a sequence number, preferably by incrementing a running total, the sequence in this case being a series of natural numbers. The increment need not be the unity value, and the step between adjacent numbers in the sequence can be two or three, or any suitable value. In the general case, the verification computer stores a value associated with the last match and generates the next expected value from it in accordance with a predetermined algorithm, for example the running total of matches or the generation of a random number from the running total using a pseudo random number generator, which may be in the form of a series of shift registers with feedback as is known in the art or in the form of a stored list of numbers which themselves may have been generated by such an arrangement or may have been obtained by a truly random process, this last form of random numbers being appropriate where the passwords for the user device are previously generated and stored in the device. Where the predetermined algorithm is a linear function then the next expected value can be considered to be obtained directly from the value for the last match, but where the algorithm includes a non-linear function such as the random number generator then the expected value can be considered to be obtained indirectly from the value for the last match.

The username may be stored in the user device and provided directly to the verification computer in conjunction with the offered password.

CLAIMS

1. A method of identifying a user comprising the steps of communicating to a verification computer a public username and an offered password, the offered password being provided by a user device in the possession of the user and being or having been generated in accordance with a first predetermined algorithm having an input formed by a static variable, utilising in the verification computer the communicated username either to provide an expected password and to compare the communicated offered password with the expected password to identify the user upon the occurrence of a match, the expected password being or having been generated in accordance with the first predetermined algorithm with an expected value of the static variable, or to process the communicated offered password in accordance with the inverse of the first predetermined algorithm to obtain the value of the static variable corresponding to the communicated offered password and to compare the obtained value with the expected value of the static variable to identify the user upon the occurrence of a match, the expected value of the static variable of the utilising step being or having been generated directly or indirectly from the expected value corresponding to the last-occurring match in accordance with a second predetermined algorithm.

2. A method as claimed in claim 1, wherein the second predetermined algorithm is or comprises a stepping function which steps the expected value corresponding to the last-occurring match to the next value in a predetermined sequence, herein referred to as sequence numbers.

3. A method as claimed in either claim 1 or claim 2, wherein the offered password is either generated, or retrieved from a stored list of previously generated passwords, in response to receipt of a command signal by the user device and in accordance with the offered value of the

static variable corresponding to the offered password being or having been generated directly or indirectly in accordance with the second predetermined algorithm from the value corresponding to the last-occurring offered password provided by the user device.

4. A method as claimed in claim 3, when the verification computer comprises a stored list of expected passwords previously generated with the second predetermined algorithm providing sequence numbers as the static variable input to the first predetermined algorithm, and the step of providing the expected password comprises retrieving the password at the address constituted by the expected value of the static variable.

5. A method as claimed in claim 3, when the user device comprises a stored list of offered passwords previously generated with the second predetermined algorithm providing sequence numbers as the static variable input to the first predetermined algorithm, and the step of providing an offered password comprises retrieving the password at the address constituted by a sequence number generated by the second predetermined algorithm in response to a received command signal.

6. A method as claimed in claim 3, including the prior steps, upon authorisation of a new user, of generating a respective random number, and generating the respective list of passwords to be stored in a user device to be issued to the newly authorised user starting with the random number as the first of the sequence numbers, entering the generated list of passwords into a store in the user device with the first password so generated being stored in the first location of the store, and issuing the user device to the newly authorised user; wherein the generation of the expected static variable by the verification computer is constituted by entering the respective random number as the first of the

sequence numbers in a respective store and replacing the current contents of the respective store with the next sequence number on each match of passwords for the respective user; and wherein an offered password is retrieved from the location in the stored list of passwords in the user device corresponding to a running total of received command signals.

7. A method as claimed in any one of claims 3 to 6, wherein the command signal is constituted by a predetermined input to the user device.

8. A method as claimed in claim 7, wherein said predetermined input is actuation of one or more specific keys of the user device.

9. A method as claimed in claim 7, wherein said predetermined input comprises the entering of a first personal identification number (PIN) into the user device which matches a stored PIN therein.

10. A method as claimed in claim 7, wherein said predetermined input comprises the entering of a username which matches a stored username therein.

11. A method as claimed in any one of claims 1 to 10, wherein the user device provides the offered password via a display, and including entering a second personal identification number (PIN) into the user device and enabling the display upon matching the entered second PIN with a PIN stored in the user device.

12. A method as claimed in claim 11, when dependent on claim 9, wherein the first PIN constitutes the second PIN .

13. A method as claimed in any one of claims 1 to 12, wherein the first predetermined algorithm has a further input formed by a user-specific code.

14. A method as claimed in claim 13, including storing the user-specific code in the verification computer, and retrieving the user-specific code for generating an expected password upon communication to the verification computer of a third personal identification number (PIN) which matches a stored PIN therein.

15. A method as claimed in claim 14, including storing in the user device a predetermined code for use as the further input, and storing the predetermined code in the verification computer, wherein said predetermined input comprises the entering of a further PIN into the user device which matches a corresponding PIN stored in the user device, and directly or indirectly comparing the communicated password in the verification computer with an expected password generated with the predetermined code as the further input, and actuating an alarm upon the occurrence of a match.

16. A method as claimed in any one of claims 9, 12, 14, and 15, wherein the entering of any PIN other than said first PIN and, as the case may be, said further PIN, causes the user device to provide a password from a predetermined set of passwords not generated in accordance with the first predetermined algorithm and which the verification computer will recognise as resulting from unauthorised use of the user device and take no action.

17. A method as claimed in claim 16, wherein the user device delays the provision of the password from said predetermined set with progressively increasing delay for each such unauthorised use of the user device.

18. A method as claimed in claim 13, including the steps of previously modifying the user-specific code in accordance with a fourth personal identification number (PIN) and a third predetermined algorithm, storing the PIN-modified user-specific code in the verification computer, communicating a

fifth PIN to the verification computer, and utilising the inverse of the third predetermined algorithm and the fifth PIN to produce a code for use as said further input to the first predetermined algorithm, the correct user-specific code being produced only when the fifth PIN is the same as the fourth PIN.

19. A method as claimed in any one of claims 14 to 18, wherein the user communicates the third PIN or the fifth PIN, as the case may be, directly to the verification computer.

20. A method as claimed in any one of claims 14 to 18, wherein the third PIN or the fifth PIN is communicated to the verification computer from the user device.

21. A method as claimed in claim 20, wherein the user device modifies the password to be offered in accordance with the third PIN or the fifth PIN and a fourth predetermined algorithm, and the step of communicating the PIN to the verification computer is constituted by communicating the PIN-modified password to the verification computer and utilising therein the inverse of the fourth predetermined algorithm to obtain the communicated PIN.

22. A method as claimed in any one of claims 1 to 13, wherein the expected and offered passwords are generated as modified passwords in accordance with a fifth predetermined algorithm and a respective sixth and seventh personal identification numbers (PIN), and the verification computer identifies the user on the basis of the comparison of the PIN-modified expected password with the communicated PIN-modified offered password.

23. A method as claimed in any one of claims 20 to 22, wherein the third, fifth or seventh PIN, as the case may be, is stored in the user device.

24. A method as claimed in any one of claims 20 to 22, wherein the user enters the third, fifth or seventh PIN, as the case may be, into the user device.

25. A method as claimed in either claim 23 or claim 24, when claim 13 is dependent on any one of claims 9, 11 and 12, and claim 21 is dependent on any one of claims 9 and 11 to 13, wherein the third, fifth or seventh PIN is constituted by the first or second PIN, as the case may be.

26. A method as claimed in any one of the preceding claims, together with the further steps, for identifying the verification computer to the user, of providing the next following expected password upon the occurrence of matching passwords, and comparing the next following expected password with the next following offered password provided by the user device.

27. A method as claimed in claim 26, including communicating the next following password directly to the user device, comparing it with the next following offered password in the user device and providing an indication of a match to the user.

28. A method as claimed in any one of the preceding claims, wherein, if the result of direct or indirect comparison of passwords is not a match, the verification computer deems the offered and expected static variables to be out of synchronism and makes up to a predetermined number of further comparisons with successive following expected static variables to attempt to resynchronise the expected static variable with the offered static variable.

29. A method of verifying a user comprising the steps of communicating to a verification computer a public username and offered verification information, herein referred to as OVI, utilising in the verification computer the communicated

username to provide expected verification information, herein referred to as EVI, and comparing the communicated OVI directly or indirectly with the EVI, the verification computer accepting the user as identified if the comparison result is a match, the OVI being provided by a user device in the possession of the user and being obtained in accordance with a first predetermined process, and the EVI being obtained in accordance with a second predetermined process, the method being characterised by either the OVI being or having been generated from static information associated with verification information last provided by the user device, and the EVI being or having been generated from static information associated with verification information last used by the verification computer successfully to identify the user.

30. A user device for use in a personal identification system, the device comprising means for storing a list of passwords, means responsive to receipt of a command signal for retrieving, in use, a password from the storing means, and means for providing the retrieved password, in use, to a verification computer of the system.

31. A device as claimed in claim 30, wherein the retrieving means comprises means for counting the received command signals and means responsive to the counting means for addressing the storing means.

32. A device as claimed in claim 31, wherein the addressing means provides an address pointer which is equal to the current count of the counting means.

33. A user device for use in a personal identification system, the device comprising means for generating in response to receipt of a command signal a password to be offered, in use, to a verification computer of the system, and means for providing the generated password, in use, to

the verification computer, the generating means being arranged to generate the password in accordance with a first predetermined algorithm having an input formed by a variable.

34. A device as claimed in claim 33, wherein the generating means is arranged to generate the password in accordance with a user-specific code forming a further input to the first predetermined algorithm.

35. A device as claimed in either claim 33 or claim 34, wherein the generating means comprises means for counting received command signals and for supplying the current count as the variable input for the first predetermined algorithm.

36. A device as claimed in either claim 33 or claim 34, wherein the generating means comprises means for counting received command signals and is arranged to generate the variable input in accordance with a second predetermined algorithm having an input formed by the current count of the counting means.

37. A device as claimed in any one of claims 30 to 36, and comprising key means operable by a user to provide a signal constituting said command signal.

38. A device as claimed in any one of claims 33 to 36, comprising first input means for plural character input, first means for storing a character stream, and first means responsive in use to the input of a character stream matching a first predetermined character stream stored in the first storing means for providing a signal which signal constitutes the command signal.

39. A device as claimed in any one of claims 30, 33 and 34, comprising input means operable by a user for inputting a command signal comprising a number, and wherein the retrieving means or the generating means, as the case may be,

is responsive to the command signal which it utilises as an address pointer or as the variable input.

40. A device as claimed in any of claims 30 to 39, wherein the providing means comprises means for displaying the retrieved or generated password.

41. A device as claimed in claim 37, wherein the displaying means is responsive to an enabling signal and comprises second input means for plural character input, second means for storing a character stream, and second means responsible in use to the input of a character stream matching a second predetermined character stream stored in the second storing means for providing a signal, which signal constitutes the enabling signal.

42. A device as claimed in claim 41, when claim 40 is dependent on claim 38, wherein the second input means, the second means for storing, and the second means for providing a signal, are respectively constituted by the first input means, the first means for storing, and the first means for providing a signal.

43. A device as claimed in any one of claims 30 to 42, wherein the providing means comprises means for communicating, in use, directly with the verification computer.

44. A device as claimed in any one of claims 30 to 43, comprising means for modifying a password to be provided in accordance with a predetermined algorithm having as inputs the password and a third predetermined character stream.

45. A device as claimed in claim 44, comprising a third storing means for storing in use the third predetermined character stream, and wherein the modifying means is arranged

to retrieve the third predetermined character stream from the third storing means.

46. A device as claimed in claim 45, when claim 44 is dependent on any one of claims 38, 41 and 42, wherein the third storing means is constituted by the first storing means or the second storing means, as the case may be.

47. A verification computer for use in a personal identification system, comprising input means for receiving plural characters, means responsive to the receipt via the input means of a first predetermined character string, constituting a predetermined user name, for providing an expected password, means responsive to the receipt via the input means of a second predetermined character string, at least a part of which constitutes an offered password, for comparing the offered and expected passwords and for providing an indication in the event of a match, and means for counting said indications, and wherein the providing means comprises means for storing a list of passwords and means responsive directly or indirectly to the current count of the counting means for retrieving, in use, a password from the storing means.

48. A computer as claimed in claim 47, wherein the retrieving means provides an address pointer in accordance with a predetermined algorithm having an input formed by the current count of the counting means.

49. A computer as claimed in claim 48, wherein the retrieving means comprises a look-up table generated in accordance with the predetermined algorithm and is arranged to address the table with the current count to retrieve the corresponding address pointer.

50. A verification computer for use in a personal identification system, comprising input means for receiving

plural characters, means responsive to the receipt via the input means of a first predetermined character string, constituting a predetermined user name, for providing an expected password, means responsive to the receipt via the input means of a second predetermined character string, at least a part of which constitutes an offered password, for comparing the offered and expected passwords and for providing an indication in the event of a match, and means for counting the indications, and wherein the providing means comprises means for generating the expected password in accordance with a predetermined algorithm having a variable input formed directly or indirectly by the current count of the counting means.

51. A computer as claimed in claim 50, wherein the generating means is arranged to generate the password in accordance with a user-specific code forming a further input to the predetermined algorithm.

52. A computer as claimed in claim 51, wherein the providing means comprises means for storing the user-specific code and a corresponding predetermined character stream, and is arranged to retrieve and supply the user-specific code to the generating means upon an offered character string matching the corresponding predetermined character string.

53. A computer as claimed in claim 52, wherein the offered character string is received via the input means.

54. A computer as claimed in claim 52, wherein the providing means includes means for processing the second predetermined string in accordance with a further predetermined algorithm to produce the offered password and the offered character string.

55. A computer as claimed in any one of claims 50 to 54, wherein the providing means is arranged to provide the

variable input indirectly in accordance with a predetermined algorithm having an input formed by the current count of the counting means.

56. A computer as claimed in claim 55, wherein the providing means comprises a look-up table generated in accordance with the predetermined algorithm and is arranged to address the table with the current count to retrieve the corresponding variable value.

57. A computer as claimed in any one of claims 47 to 56, wherein the input means is arranged for direct communication from a user device forming part of the system.

58. A computer as claimed in any one of claims 47 to 57, wherein the providing means comprises output means for outputting character strings.

59. A computer as claimed in claim 58, wherein the output means comprises a visual display.

60. A computer as claimed in either claim 58 or claim 59, wherein the output means is arranged for direct communication with a user device forming part of the system.

61. A computer as claimed in any one of claims 58 to 60, wherein the providing means is arranged to respond to said indication to provide the next following expected password corresponding to the next successive count value and to supply said next following expected password to the output means.

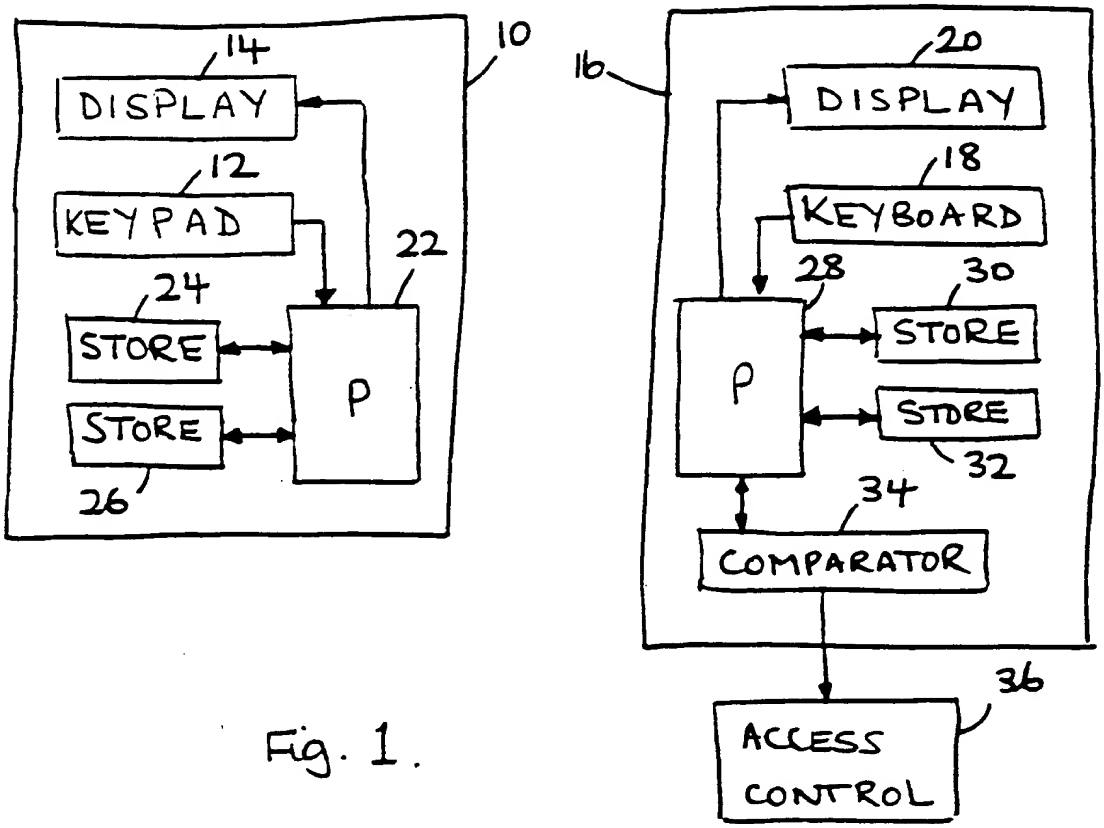

14
10
DISPLAY
12
KEYPAD
22
24
STORE
P
STORE
26
16
20
DISPLAY
18
KEYBOARD
28
30
STORE
P
STORE
32
34
COMPARATOR
36
ACCESS CONTROL

Fig. 1.

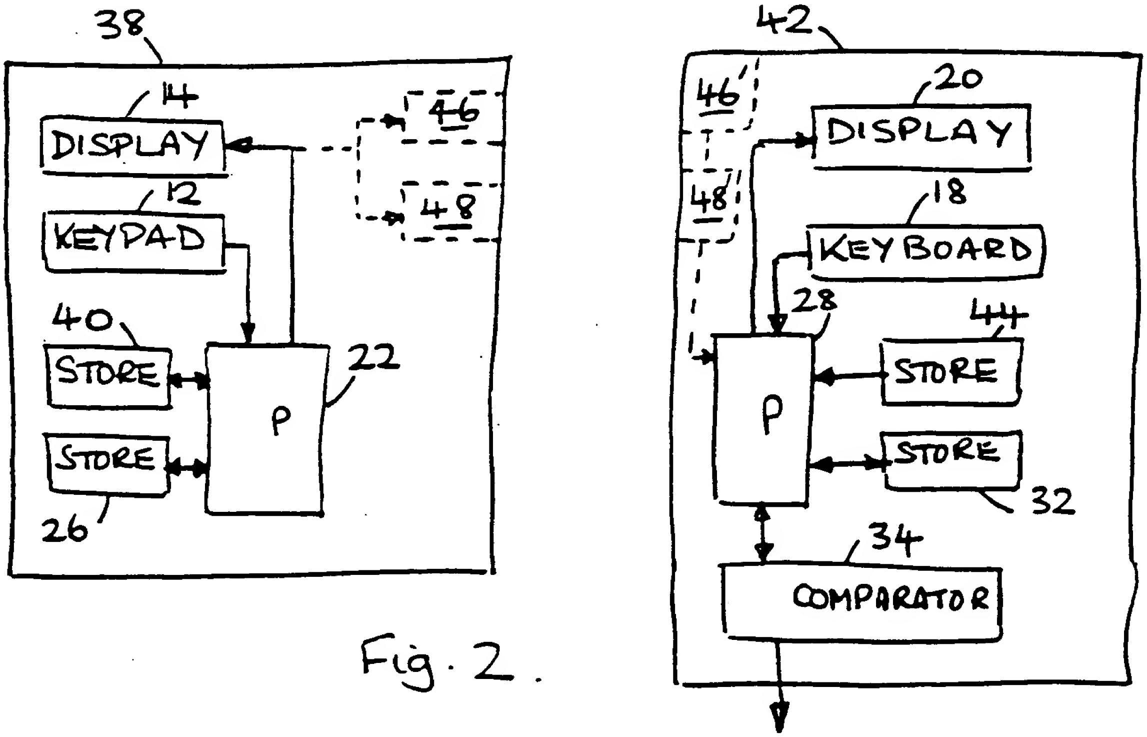

38
14
DISPLAY
46
12
KEYPAD
48
40
STORE
22
P
STORE
26
42
46
20
DISPLAY
48
18
KEYBOARD
28
44
STORE
P
STORE
32
34
COMPARATOR

Fig. 2.

THIS PAGE BLANK (USPTO)

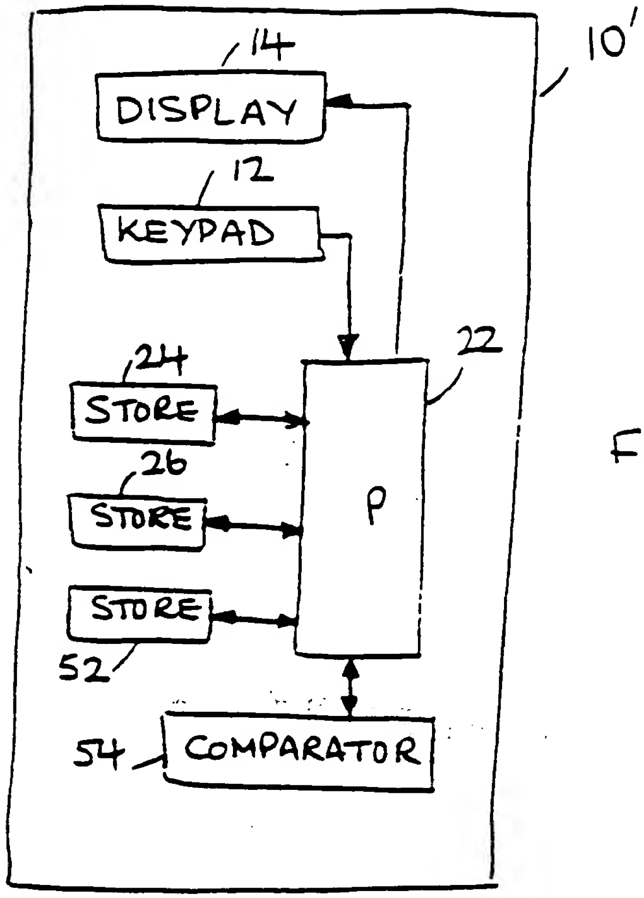

10'
14
DISPLAY
12
KEYPAD
22
24
STORE
26
STORE
p
STORE
52
54
COMPARATOR

Fig. 3.

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 94/02250

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US,A,5 130 519 (GEORGE BUSH ET.AL.) 14 July 1992 see column 2, line 17 - line 56 see column 4, line 38 - column 5, line 59; claims 1-3; figures 1-4 ---	1,3-5, 7-10, 13-16, 22-30, 32-34, 38,39, 47,49, 51-58
A	WO,A,85 03787 (PETER WHITE) 29 August 1985 see abstract; claims; figures --- -/--	1-3, 5-10,26, 29-39, 47-54

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search 27 January 1995	Date of mailing of the international search report - 8. 02. 95
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+ 31-70) 340-3016	Authorized officer Guivol, O

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 94/02250

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,5 060 263 (BOSEN ET.AL.) 22 October 1991 see column 7, line 12 - column 13, line 43; claims 1-10; figures 3,6,9 ---	1-14, 22-61
A	WO,A,92 07436 (SECURITY DYNAMICS TECHNOLOGIES) 30 April 1992 see claims 1-21; figure 3 ---	1,3-14, 18-27, 29,33,47
A	FR,A,2 681 165 (GEMPLUS CARD INTERNATIONAL) 12 March 1993 see abstract; claims 1-7; figure 3 ---	1,3-14, 29,30,47
A	US,A,4 605 820 (CAMPBELL,JR.) 12 August 1986 see column 2, line 33 - column 7, line 50; figures 1-12 ---	1-14, 18-61
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 36, no.5, May 1993 ARMONK, NEW YORK, USA, pages 309-312, XP 000409003 'Alert PIN for Personal Banking Terminals' ---	15,16
A	GB,A,2 070 306 (OMRON TATEISI ELECTRONICS) 3 September 1981 see abstract; claims 1-3; figures 1-6 ---	15-17
A	DE,A,39 04 215 (ASEA BROWN BOVERI) 31 August 1989 see the whole document ---	1,6-12, 40,59
A	FR,A,2 496 294 (THOMSON-CSF) 18 June 1982 see page 3, line 5 - page 5, line 32; claims 1-5 ---	1-3, 5-13, 22-27, 29, 31-39, 43-46, 50-55
A	GB,A,2 261 538 (THE GOVERNOR AND COMPANY OF THE BANK OF SCOTLAND) 19 May 1993 see page 7, line 17 - page 11, line 3; claims 1-9 ---	1-4,6
A	FR,A,2 600 188 (BULL CP8) 18 December 1987 see the whole document --- -/--	1

1

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 94/02250

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE,A,34 11 570 (MONIKA KÜBLER) 7 November 1985 see page 4, line 1 - line 34 see page 6, line 1 - page 7, line 34; figure 1	1,3-9
A	US,A,5 163 097 (TINA C. PEGG) 10 November 1992	
A	US,A,3 764 742 (GEORGE F. ABBOTT ET.AL.) 9 October 1973	

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte. .onal Application No
PCT/GB 94/02250

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US-A-5130519	14-07-92	US-A-	5265162	23-11-93
WO-A-8503787	29-08-85	US-A-	4630201	16-12-86
		CA-A-	1232684	09-02-88
		EP-A-	0172877	05-03-86
		JP-B-	5014298	24-02-93
		JP-T-	61501477	17-07-86
US-A-5060263	22-10-91	NONE		
WO-A-9207436	30-04-92	US-A-	5097505	17-03-92
		US-A-	5168520	01-12-92
		AU-B-	642362	14-10-93
		AU-A-	6720890	31-05-91
		AU-B-	649190	12-05-94
		AU-A-	7981691	20-05-92
		CA-A-	2094026	20-04-92
		EP-A-	0497889	12-08-92
		EP-A-	0555219	18-08-93
		JP-T-	6507277	11-08-94
		JP-T-	5503598	10-06-93
		WO-A-	9106926	16-05-91
		US-A-	5367572	22-11-94
FR-A-2681165	12-03-93	NONE		
US-A-4605820	12-08-86	NONE		
GB-A-2070306	03-09-81	JP-A-	56111967	04-09-81
		US-A-	4375032	22-02-83
DE-A-3904215	31-08-89	CH-A-	675169	31-08-90
FR-A-2496294	18-06-82	NONE		
GB-A-2261538	19-05-93	NONE		
FR-A-2600188	18-12-87	NONE		
DE-A-3411570	07-11-85	NONE		

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/GB 94/02250

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-5163097	10-11-92	NONE	
US-A-3764742	09-10-73	CA-A- 957948	19-11-74
		DE-A,B,C 2253275	05-07-73
		FR-A- 2164939	03-08-73
		GB-A- 1399020	25-06-75

THIS PAGE BLANK (USPTO)